电力监控系统现场运维安全管控系统研究

蔡豪

国网漯河供电公司　河南　漯河　462000

[摘　要]当下，电力、通讯、金融、交通等行业是让社会得以有序运行和经济平稳发展的重要支柱，其稳定性、安全性关系国计民生。随着国家对数字化转型的推进，作为国家基石的电力行业所面临的网络安全挑战愈发严苛。隔绝安全隐患，降低安全风险，建设安全防护体系，提升安全防护水平，可有力防范网络安全事件的发生，有效保障电力系统安全稳定运营和可靠供应。

[关键词]电力监控；安全管控

【DOI】10.12252/j.issn.2096-6261.2020.02.557

引言

智能化电力系统的构建和应用，信息网络的重要作用日益突出，自动化控制系统逐渐替代了传统的安放措施，为此，国家电网逐渐加强了对电力监控系统二次安防建设，由此为整个电力监控系统的安全、稳定运行打下良好基础。

1 火力发电安全风险分析

1.1火力发电特点

火力发电厂中所涉及的工艺流程复杂，一般通过大型分散控制系统（DCS）对发电过程中燃烧系统、汽水系统、电气系统三大系统的运转进行控制。这三大系统内部根据生产环节不同又分成了其他如输煤、锅炉燃烧、除尘、汽机等系统，不同生产环节适用的控制系统类别也有所不同。电厂在信息化生产运营中除了控制系统之外，还需要管理信息系统（MIS）和厂级监控信息系统（SIS）等的协调配合，依此完成企业的生产、运营和行政管理，优化电厂实时生产过程。DCS、MIS、SIS 系统，所用协议、所面向的对象和侧重点都不一样，在数字化进程中，不同系统的更新和优化带来便捷的同时，也会让系统整体更加复杂，带来更多问题。

1.2安全风险分析

传统火电厂在迈向新时期智慧电厂的转变中所面临的常见安全风险如下：边界防护薄弱：火电厂在生产过程中需要由管理系统进行协调和控制，这使得生产系统网络与管理系统网络参杂互联，让控制生产的工业控制系统网络面临来自外部信息网络的安全威胁，控制系统将更容易被入侵。传统安全难适配：火电厂生产中使用的工业控制系统对实时性和可靠性有着极高要求，跟传统信息安全产品所适配的场景不一样；同时火电生产场景中涉及的工业协议种类众多，安全产品需要对工控协议进行深度解析防护，防护难度大。网络监控能力较弱：电厂识别网络入侵行为、病毒、业务访问异常等现象的技术手段薄弱，一旦发生问题，难以追踪溯源和及时处理。存在终端安全风险：火电厂所采用的工业主机系统配置简单，系统几乎从不更新，无法及时修补系统漏洞，容易被外界入侵。控制设备存在漏洞：以往的火电厂很多采用西门子、ABB、艾默生等国外控制系统，而进口的控制系统是否存在后门和漏洞尚不掌握；传统工业控制系统本身的安全防护能力薄弱，部分控制系统或者设备本身就有的漏洞存在，一旦被外界利用，将引起巨大生产事故。生产运维风险：火电厂工控系统专业性强，需设备厂商人员来负责运维检修，但却缺乏合适的监管手段，若外部设备厂家或控制系统运维人员的个人电脑、U盘在维护时使用，会使得工作主机易被入侵和感染病毒。

2 电力监控系统网络安全智能管控中的问题

2.1网络安全防护技术水平不足

电力监控系统实际上是相对来说比较复杂的系统，其中会涉及不同方面的内容和众多的流程，若要真正意义上达到电力系统的 100% 安全性，是一项困难的任务。同时，在电力监控系统的运行过程中，有关的管理人员对于网络安全防护工作不够重视，导致整体的网络安全防护水平以及质量都比较差。而在安全防护方面的各项工作的执行效果也并不是十分理想，导致电力监控系统在实际运行的过程中会受到多重因素的影响，产生安全方面的问题和隐患。

2.2网络安全防护工作效率较低

很多负责电力监控系统网络安全防护管理的工作人员，在工作的过程中并不会更改系统中自带的一些较为简单的口令，而是会采取远程操作的方式完成相应的安全防护工作，这就可能会泄漏系统中的口令以及密码，导致电力监控系统在运行过程中面对安全方面的隐患和威胁。由于电力监控系统是复杂的系统，在实现稳定运营过程中，必须要配备专业的工作人员，使之发挥作用。目前有很多电力网络系统在运行的过程中存在系统方面的风险因素，包括设备以及系统台账之间的连接不足，导致某些机密被泄漏出去。同时，针对电力监控系统的监管工作没有得到完美的落实，有关的工作人员也并没有承担起应负的责任，导致电力监控系统在运行的过程中出现了较多的网络安全隐患，严重影响到了电力监控系统的整体质量。

2.3发电厂网络安全问题

基于计算机及网络安全原理，要做到网络安全防护的全面覆盖，发电企业的网络安全建设需要投入大量的设备和人力资源。网络安全设备类型多，功能单一，受限于发电厂工业控制终端的应用环境，无法通过单一设备的部署和应用

进行全面的网络安全防护。网络安全专业技术人力资源在各发电企业均较少，大部分网络安全人员都为非专业兼职人员，这就导致了发电厂的整体网络安全技术水平和防护能力较弱。在网络安全设备和人力资源的投入上，不是一次投入就可以获得直接效果，而是需要发电企业长期持续的投入才能取得效果。受限于国内发电厂电力监控系统针对性研究薄弱、工业控制环境复杂、网络安全防护薄弱等突出特点，开展电力监控系统网络安全一体化平台、网络架构及控制策略等关键技术研究，确保电力监控系统安全稳定运行是当前面临的重要课题。

3 电力监控系统网络安全智能管控的优化策略

3.1二次安全防护技术应用

随着信息技术以及网络技术的发展和应用，越来越多的先进技术被应用在电力监控系统二次安防过程中，如，VLAN、MPLS-VPN、数据证书等技术。其中，VLAN技术作为一种特别的虚拟局域网，不仅可以切实的降低网络移动和变化成本费用，而且还可以实现资源的最大化利用。其通过网络广播通信的方式科学的对用户群体进行划分，并通过各组别间的访问权限设置切实提升了系统的安全性；MPLS-VPN则是主要应用在电力运行和管控的交换设备或者网络路由器上，其主要是依托于IP-VPN技术，从而有效地将IP网络分解为彼此隔离的网络，进而保证了二次安防的独立以及互访需求，切实的保证隔离和互访过程中的数据安全；而数据证书技术则主要是依托于公钥而研发出的一种新型的分布式数字证书系统。譬如，程序、设备和人员证书等，此技术主要是被应用在电力系统的监控以及数据网调度等方面，切实实现对用户的身份认证户这话操作人员的行为审计，特别是数字签名等功能切实提升二次系统的安防效果。

3.2提高安全管理技术水平

在社会的发展过程中，要发挥电力监控系统中各种信息数据的作用，确保这些数据信息以及资料不被泄漏，就需要采取科学合理的信息加密技术方法。实际中，数据传输加密技术是建立安全管理系统以及提高安全管理技术水平中有效的方式，主要是采取加密钥匙以及加密算法等方式，针对电力监控信息系统进行保护，将系统中一些重要的信息转变成为看似不重要或者是用难以直接理解的符号，之后对电力监控系统安全性提供保障。在加密环节主要涉及的内容包括明文、密文以及密钥3个方面，而使用这种先进的加密数据技术，就需要确保电力监控系统运行的过程中传输信息时能够使用密钥去发送密文，之后提取信息的工作人员再通过有关的解密技术对获得的密文进行解密。密钥包括专用密钥以及公开密钥，实际中针对不同的密钥进行解密时，需要使用的技术方法都并不完全一致，但是使用的这些差异性的解密技术方法都需要应用在电力监控系统的网络安全防护管理工作中，这是它们的统一性。目前，我国的电力监控生产系统中选择的通常是纵向加密认证的装置，在实际应用的过程中要调整数据网络体系，并加强网络安全方面的系数，使用更加独特和专业的密文，尽量在不会影响到用户网络设置的前提上提高数据信息的安全性、可靠性以及完整性。通常来说，在电力监控系统的数据网络安全区域要选择纵向加密的方案，为其提供安全方面的保障，通过这种方式能够将明文变成密文，为后续数据传输工作的顺利开展做好基础。纵向加密技术所包括的内容丰富，而目前我国常用的就是 RSA 加密算法，电力系统运行时，每一个环节都需要进行严格的加密处理，从而确保系统运行的稳定性和安全性，防止在系统运行的过程中，某些关键的信息被不法分子窃取而对于系统的运行造成影响。

3.3实现电力监控系统网络安全防护全覆盖

电力监控系统网络安全的核心目标是要做到防护的全方面覆盖，但这不仅仅是通过技术手段就可以全面实现的，所以更需要加强网络安全的管理工作。加强专业人员的技术水平培训，确保发电厂配备2～3名专业的网络安全专业技术人员，取得一定计算机及网络技术方面的资质和能力；加强网络安全系统工作流程的标准化，网络安全的全面防护离不开日常管理工作的重视和规范化，建设符合电厂系统实际的网络安全排查、策略加固、病毒查杀、漏洞扫描等工作的标准化流程，定期按照拟定工作清单执行网络安全工作；加强网络安全防护数据库的建立和完善，使用大数据进行网络安全工作的细节管理，挖掘网络安全技术漏洞及加固节点的策略关键，同时也为网络安全工作做好技术备份；加强网络安全工作的资源投入，对于涉及的人力、设备和系统资源，积极申请项目资金，完善建设电力监控系统网络安全防护体系。

结束语

发展网络安全技术、建设网络安全防护体系、提升网络安全防护能力是一场需要坚持不懈的持久战。我们应进一步提高对新形势、新挑战、新任务的认识，把握工作关键方法，不断发现问题，坚持改进问题，努力开创电力网络安全与信息化工作新局面，让电力行业的安全免疫机制真正活起来，保障国家关键信息基础设施安全，为推动能源转型和电力安全发展做出新的贡献。

参考文献

[1]刘日堂，梁野，谷丰强，等.安全监视闭环管控技术在电力监控系统中的应用[J].中国科技纵横，2016（23）：3.

[2]朱昊.电力监控系统信息安全管理系统的研究与分析[J].科技创新导报，2019，16（36）：2.

[3]岳浩.电力监控系统安全防护管理与技术研究[J].科技创新与应用，2019（31）：2.